<u>Amendments to the Drawings</u>:

The attached sheets of drawings includes changes to sheets 1 and 6. These sheets, which include Figures 1 and 6, replace the original sheets 1 and 6 including Figures 1 and 6.

Attachment: Replacement Sheets
                Annotated Sheets

REMARKS/ARGUMENTS

In the final Office action dated September 14, 2005 all of the claims were rejected under 35 U.S.C. § 102. Applicant requests reconsideration of the rejection and reexamination of this application.

By this Amendment Applicant is correcting typographic errors in the specification and drawings and one of the claims. Since these amendments are of a minor nature and do not impact the true scope of the claims, Applicant respectfully requests entry of this Amendment even though the application is now under final rejection.

Applicant's Amendments to the Drawings.

Applicant has amended Figure 1 to delete the second occurrence of reference numeral 24 as shown in annotated sheet 1 in the Appendix. Applicant also notes that the box associated with the second reference numeral 24 in Figure 1 is correctly identified with reference numeral 18. That this box is associated with reference number 18 is illustrated, for example, by the Specification at page 4, lines 21 - 28 and page 5, lines 2 - 6.

Applicant has amended Figure 6 to delete duplicative use of reference numerals 100, 102, 106 and 108 that were previously used in Figure 5. Specifically, as shown in annotated sheet 6, reference numerals 100, 102, 106 and 108 have been changed to reference numerals 200, 202, 206 and 208, respectively. The portions of the specification discussing Figures 5 and 6 illustrate that reference numerals 100, 102, 106 and 108 in

Figure 5 refer to different blocks than the erroneously labeled blocks in Figure 6. See, for example, the specification at page 10, lines 27; page 11, lines 3, 16 and 17; and page 12, lines 29 - 31 and 35. A corresponding amendment has been made to the specification as set forth below so that the new reference numerals 200, 202, 206 and 208 in Figure 6 are also referenced in the specification.

In view of the above, Applicant submits that no new matter has been added by these amendments. Moreover, as these are relatively minor amendments that do not affect the scope of the claims, Applicant respectfully requests entry of this drawing amendment even though a final action has been issued for this application.

Applicant's Amendments to the Specification.

Applicant has amended the specification to correct typographical errors or inadvertent omissions. Applicant will discuss each of these amendments in turn.

The amendment in the paragraph beginning at page 4, line 20 that adds reference numeral 12 is supported, for example, by the specification at page 4, lines 21 - 22. This portion of the specification describes how signals 14 and 16 are passed from device 10 to a second device. Figure 1 illustrates that this second device is labeled using reference numeral 12.

The amendment in the paragraph beginning at page 4, line 20 that adds reference numeral 18 is supported, for example, by the specification at page 4, lines 21 - 28 and page 5, lines 2 - 6. The first cited portion of the specification states that the

parameter concealment logic block may receive the signal 14 and 16 and generates signal 20. The second cited portion of the specification states that the parameter concealment logic block may include control logic block 28 and an interface operation logic block 26). Figure 1 illustrates that the above description refers to the block labeled using reference numeral 18.

The amendment in the paragraph beginning at page 5, line 29 relating to the second key table module 318 is supported, for example, by the specification at page 5, lines 33 and 34. This portion of the specification describes how this key table module generates a second key signal 324. Figure 7 illustrates that the block 318 provides the signal 324. In addition, the specification at page 5, line 18 shows that the block 318 is the second key table module.

The amendment in the paragraph beginning at page 7, line 24 corrects an obvious typographical error.

The amendments on page 12 are discussed above in conjunction with the amendments to Figure 6.

In view of the above, Applicant submits that no new matter has been added by these amendments. Moreover, as these are relatively minor amendments that do not affect the scope of the claims, Applicant respectfully requests entry of these amendments of the specification.

Applicant's Amendments of Claim 7

Applicant has amended claim 7 to correct a typographical error. Applicant submits the intended language of the claim was

clear from the context of claim 7. Moreover, Applicant believes claim 7 has been interpreted by the Office in a manner consistent with the amendment.

In view of the above, Applicant submits that this amendment does not materially affect the scope of the claims. Accordingly, Applicant respectfully requests entry of this amendment of claim 7.

Applicant's Response to the 35 USC § 102 Rejection

Claims 1 - 10 were rejected under Section 102 as being anticipated by Brown, et al., U.S. Patent No. 6,732,179 (hereafter "Brown"). Applicant respectfully submits that claims 1 - 10 are patentable over Brown.

Brown discloses a cable modem authentication system that enables a user (via a client 112) to access certain services via a walled garden proxy server ("WGPS") 414. To this end, the system includes a gateway server ("GS") 416 that provides a ticket 800 that the client 112 presents to the WGPS 414 to gain access to a service. At column 12, lines 15 - 20, Brown discloses that the GS 416 either encrypts the entire ticket 800 or the portion of the ticket defining user access rights 816. At column 10, lines 11 - 25, Brown discloses that a keymaster provides encryption keys to the GS 416 and the WGPS 414. At column 12, lines 15 - 20, Brown discloses that the GS 416 sends the ticket to the client 112 and that the client 112 cannot modify or decrypt the encrypted ticket. At column 12, lines 39 - 43 Brown discloses that the client sends the encrypted ticket to the WGPS 414 in an authentication header. At column 12,

lines 46 - 55 Brown discloses that the WGPS 414 uses a time stamp to determine a secret key that is used to decrypt the encrypted ticket. At column 12, lines 56 - 62 Brown discloses that the WGPS 414 examines the access rights bits 812 from the decrypted ticket.

Applicant respectfully submits that Brown does not teach or suggest the limitations of claim 1. For example, claim 1 recites, in part: "transforming by the first device a portion of the control signal with the parameter signal to generate an encrypted parameter signal and control signal; and generating by the second device a destination parameter signal using the control signal and the encrypted parameter signal and control signal."

Accordingly, claim 1 relates to a method that may be used to securely transfer data (e.g., a parameter signal) and control information (e.g., a control signal) from one device to another. The first device encrypts the data and a portion of the control information and sends the encrypted result along with the entire control information (in unencrypted form)) to the second device. The second device may then generate the desired data (e.g., a destination parameter signal) using the encrypted result and the control information. In addition, provisions may be made to ensure that the received unencrypted control information is valid since it may be checked against the portion of the control information that was encrypted (see, e.g., claim 6).

As best understood, the Office action contends that the ticket 800 of Brown corresponds to the claimed control signal. However, neither this aspect of Brown nor any other aspect of

Brown teaches nor suggests the limitations recited above. For example, claim 1 is directed to a method where an entire control signal and a portion of the control that has been encrypted (along with a parameter signal) are transmitted from a first device to a second device. Brown does not teach or suggest, however, that the entire ticket in unencrypted form and a portion of the ticket that is encrypted are both transmitted. Rather, Brown states that the entire ticket may be encrypted and sent. Alternatively, Brown states that a portion (the access right bits 816) of the ticket may be sent, but does not state that this portion of the ticket is also sent in an unencrypted form at the same time. Hence, in this second scenario, the entire ticket is not sent in unencrypted form along with an encrypted portion.

Moreover, Brown does not teach or suggest that a parameter signal and a portion of a control signal are transformed to generate an encrypted parameter signal and control signal. Rather, Brown only refers to encryption of the control signal or a portion of the control signal.

Moreover, Brown does not teach or suggest using an original unencrypted control signal and encrypted parameter and control signal (where the encrypted control signal is a portion of the original control signal) to generate a destination parameter signal. Rather, as noted in the referenced sections above, the WGPS 414 only receives the ticket encrypted as discussed above. Thus, the WGPS either receives the entire encrypted ticket or a portion of the ticket unencrypted and a portion of the ticket encrypted.

In view of the above differences between claim 1 and Brown, Applicant submits that claim 1 is patentable over Brown.

Claim 2 recites, in part "generating by the first device a first key signal using the control signal." The claim thus recites that the first device (as defined in claim 1) generates the key. This limitation is not taught or suggested by Brown. Brown discloses as cited above that a keymaster 442 provides keys to the GS 414. Brown does not say, however, how this is done. The client 112 does not generate a key. Hence, Brown does not teach or suggest a first device as claimed that generates a key using the control signal. Accordingly, Applicant submits that claim 2 is patentable over Brown.

Claim 4 recites, in part "transmitting by the first device to the second the key index signal and the key variable signal." The only mention of an key index by Brown found by Applicant is at column 10, lines 24 - 25. Brown does not teach or suggest, however, that this key index may be transmitted as claimed.

Claim 4 also recites, in part "generating by <u>the second device</u> an <u>intermediate key signal</u> using the <u>key index</u> signal and a key table; and generating by the second device the <u>second key signal using the intermediate key signal</u> and the key variable signal." Brown does not teach or suggest generates a second key signal using a first (intermediate) key signal. Rather, Brown discloses that the keymaster 442 generates keys. No mention is made of any other key signal as claimed that is used by the key master. Brown also discloses that the WGPS determines a key using a timestamp. This is not the same process as the claimed method where an intermediate key is generated using a indes and

another key is generated using the intermediate key and another signal. Accordingly, Applicant submits that claim 4 is patentable over Brown.

Brown makes no mention of a hash function. Accordingly, Applicant submits that claims 5 and 10 are patentable over Brown.

Claim 6 recites, in part "comparing by the second device the inversely transformed control signal portion to a portion of the received control signal." Brown does not teach or suggest that the WGPS compares a portion of the unencrypted ticket with the encrypted ticket. Accordingly, Applicant submits that claim 6 is patentable over Brown.

Claim 7 relates to an apparatus that may securely receive and use a concealed parameter. The apparatus generates the desired data (e.g., a destination parameter signal) using a control signal and an encrypted parameter signal and control signal. Claim 7 recites, in part: "an interface operation logic block operably coupled to the control signal block to generate a destination parameter signal using the control signal and the encrypted parameter signal and control signal." As discussed above in conjunction with claim 1, Brown does not teach or suggest that a parameter signal and a portion of a control signal are transformed to generate an encrypted parameter signal and control signal. Accordingly, Applicant submits that claim 7 is patentable over Brown.

Regarding claims 8 and 9, Brown does not disclose the use of indexed transformation keys or intermediate keys (as

discussed above). Accordingly, Applicant submits that claims 8 and 9 are patentable over Brown.

CONCLUSION

In view of the above remarks it is submitted that the claims are patentably distinct over the cited references and that all the rejections to the claims have been overcome. Reconsideration and reexamination of the above Application is requested.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By _____

Stephen D. Burbach
Reg. No. 40,285
626/795-9900
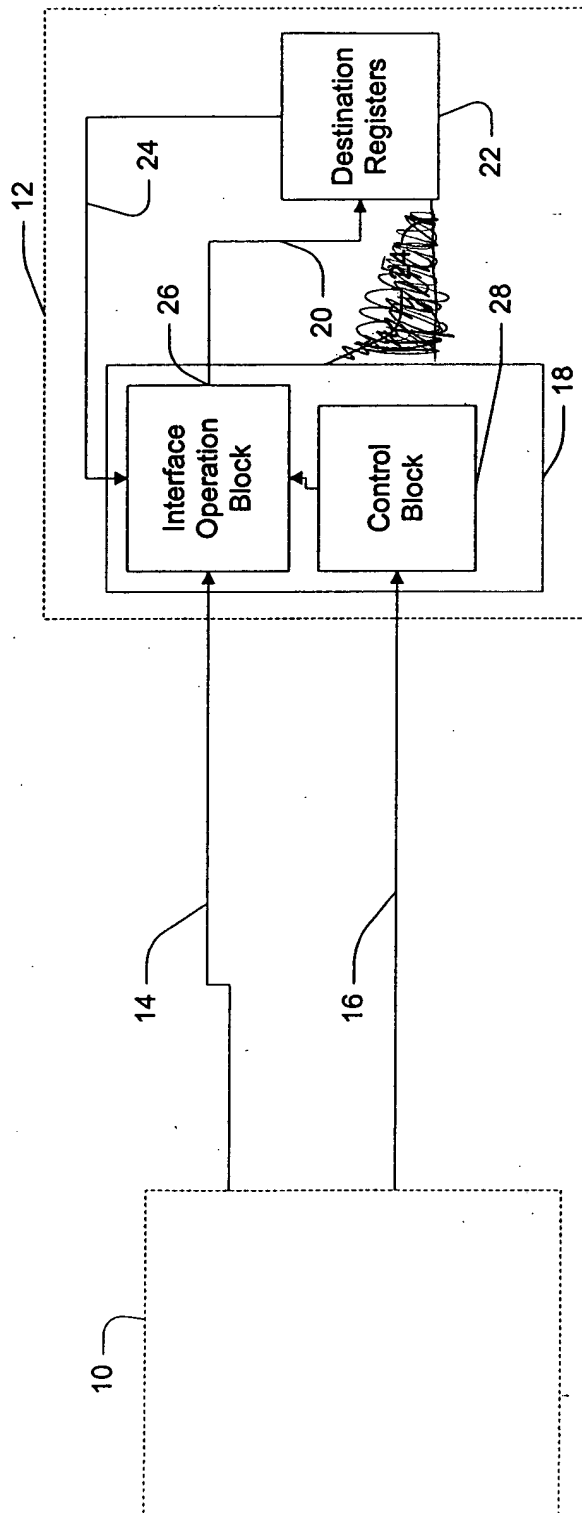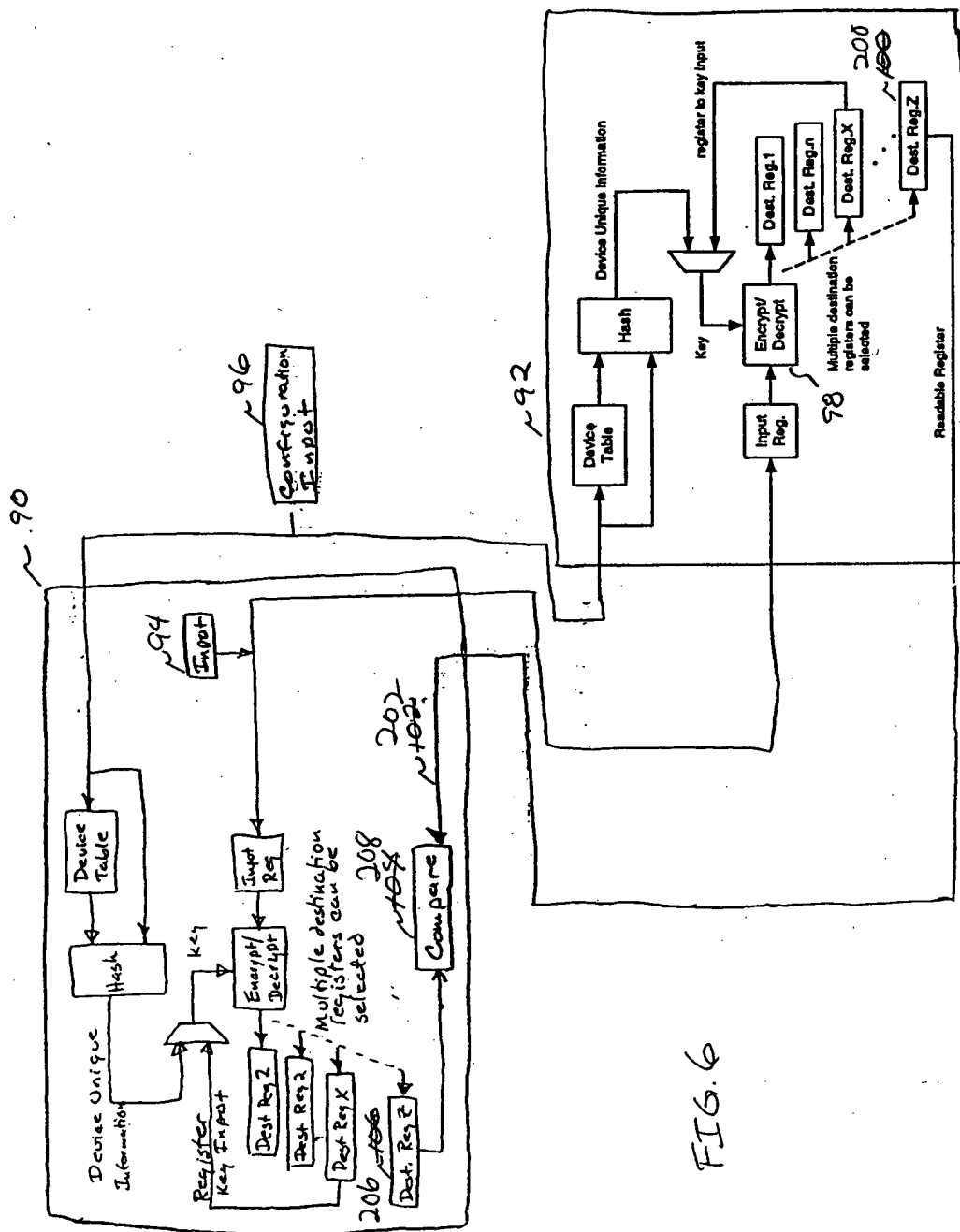
SDB/vsj
SDB PAS627470.1-*-06/28/05 6:25 PM

FIG. 1

FIG. 6